



# MobileIron Access Cookbook

## Access with SuccessFactors and Okta

**Revised: 03 January 2017**



## Contents

Overview.....	3
Prerequisites.....	3
Configure the Okta environment .....	4
Configuring SuccessFactors and Okta with MobileIron Access .....	7
Register Sentry to Access .....	7
Configure Access to create a Federated Pair .....	7
Configure the Okta environment with MobileIron Access.....	8
Configure the SuccessFactors environment with MobileIron Access .....	9
Verification .....	11



# Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as SuccessFactors is federated with an identity provider such as Okta for authentication. The user gets authenticated by Okta and obtains a token for accessing applications in a cloud environment, such as SuccessFactors. This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with SuccessFactors in a cloud environment.

## **Disclaimer:**

This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.

# Prerequisites

- Ensure that you have a working setup of native federation for SuccessFactors and Okta in your environment.
- Verify that you have the metadata files for Successfactors and Okta.

- **Okta (IDP) Metadata Files**

Download the metadata files for Okta (IdP)

Perform the steps 1 to 10 in the

- [Configure the Okta environment](#) section.



General **Sign On** Import Assignments

---


Settings Edit

**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

SAML 2.0

Default Relay State

 **SAML 2.0** is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

- **SuccessFactors (SP) Metadata Files**

Download the metadata files for SuccessFactors (SP)

➤ **Tenant ID:**

[https://salesdemo4.successfactors.com/login?company=<your\\_company>](https://salesdemo4.successfactors.com/login?company=<your_company>)

➤ **EntityID:** [https://www.successfactors.com/<your\\_company>](https://www.successfactors.com/<your_company>)

➤ **Assertion Consumer Service URL:**

[https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?<your\\_company>](https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?<your_company>)

## Configure the Okta environment

Configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

### **Procedure**

1. Login to Okta with admin credentials using the sign-in URL received in the activation mail.
2. Select **Admin >Directory > People**.
3. Select **Add Person > Fill details > Save details**.

**Note:** The email id should be same as that of SuccessFactors.



4. On the **Application** tab, click **Add Application**.
5. In the **Create a New Application Integration** window, select **SAML 2.0** radio button. Click **Create**.
6. Under the **General Setting** tab, enter the **Application name** and click **Next**.
7. In SAML settings, enter the Audience URL, Name ID format, and Application username and click **Show Advanced Settings**.
8. Enter the configuration values as shown in the below screen and click **Next**.

Response ?	Unsigned
Assertion Signature ?	Signed
Signature Algorithm ?	RSA - SHA256
Digest Algorithm ?	SHA-256
Assertion Encryption ?	Unencrypted
Enable Single Logout ?	<input type="checkbox"/> Allow application to initiate Single Logout
Authentication context class ?	PasswordProtectedTransport
Honor Force Authentication ?	Yes
SAML Issuer ID ?	http://www.okta.com/\${org.externalKey}

9. Configure the feedback settings as below and click **Finish**.

### 3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

**i** The optional questions below assist Okta Support in understanding your app integration.

App type ?  This is an internal app that we have created

10. Click **Applications** and select the application that you created. Click **Sign On** and download the identity provider metadata.
11. Click **Directory > People > Add Person** and create a **User**.
12. On the **Applications** tab, select **Assign Applications**.



13. Select the **Application** and the **User** and click **Next**.
14. Click **Confirm Assignment**.



# Configuring SuccessFactors and Okta with MobileIron Access

You must perform the following tasks to accomplish the configuration between SuccessFactors and Okta:

- [Register Sentry to Access](#)
- [Register Sentry to Access](#)
- [You must](#) register Sentry to Access to fetch the latest configuration from Access.

## Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

## Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.  
*(config)#accs registration https://<FQDN of Access server><Admin Username of Access Server>*
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action > Assign**.
5. Click **OK**.
6. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

*(config)# accs config-fetch update*

**Note:** All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

- [Configure Access to create a Federated Pair](#)
- [Configure the Okta environment with MobileIron Access](#)
- [Configure the SuccessFactors environment with MobileIron Access](#)

## [Register Sentry to Access](#)

You must register Sentry to Access to fetch the latest configuration from Access.

## Prerequisite



Verify that you have registered Sentry earlier. If so, then do not perform this step.

### **Procedure**

7. **Clish** Sentry. In the configuration mode, execute the following command for registration.  
*(config)#accs registration https://<FQDN of Access server><Admin Username of Access Server>*
8. Enter the **Tenant password** and complete the registration.
9. In **Access**, click the **Sentry** tab.
10. Select the appropriate Sentry instance, then click **Action > Assign**.
11. Click **OK**.
12. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

*(config)# accs config-fetch update*

**Note:** All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

### **Configure Access to create a Federated Pair**

You must configure Access to select your service provider and the identity provider to create a federated pair.

### **Procedure**

1. In Access, click **Profile > Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. The other fields retain their default values. Click **Save**.
3. Click **Profile > Federated Pairs > Add New Pair**.
4. Select **SAP SuccessFactors** as the service provider.
5. Enter the following details:
  - Name
  - Description
  - Select the **Access Signing Certificate** or use the **Advanced Options** to create a new Access Signing Certificate.
  - Enter the Entity ID, and Assertion Consumer Service URL for SuccessFactors. See [Prerequisites](#).
  - (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN. See *Appendix* in the *MobileIron Access Guide* at <https://support.mobileiron.com/docs/curent/accs>.
6. Click **Next** and select **Okta** as the identity provider.





7. Select the **Access Signing Certificate** or use the **Advanced Options** to create and upload a new self-signed Access Signing Certificate.
8. **Add** the IdP metadata or **Upload** the IdP metadata file that you downloaded in [Prerequisites](#).
9. Click **Done**.
10. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
11. Click **Publish** to publish the profile.

## Configure the Okta environment with MobileIron Access

### Procedure

1. Login to Okta with admin credentials.
- Click **Application** and select the application that you created in the
2. [Configure the Okta environment](#) section.
  3. On the **General** tab, click **Edit SAML Settings** and click **Next**.
  4. Extract the service provider entity ID from SP proxy metadata file and configure the settings as shown below:

The screenshot shows the 'Edit SAML Integration' page in Okta. The 'Configure SAML' tab is active. The 'SAML Settings' section is expanded to show the 'GENERAL' tab. The following settings are visible:

- Single sign on URL:**   Use this for Recipient URL and Destination URL  Allow this app to request other SSO URLs
- Audience URI (SP Entity ID):**
- Default RelayState:**  If no value is set, a blank RelayState is sent.
- Name ID format:**
- Application username:**

[Show Advanced Settings](#)



## Configure the SuccessFactors environment with MobileIron Access

### Procedure

1. Login to SAP SuccessFactors instance and click **Single Sign-On (SSO)** settings. Extract the **SAML Issuer, Certificate, Global Logout Service URL (Logout Request destination), Single Sign On** redirect service location from the metadata file that you downloaded in the Step 10 of **Register Sentry to Access**

You must register Sentry to Access to fetch the latest configuration from Access.

### Prerequisite

Verify that you have registered Sentry earlier. If so, then do not perform this step.

### Procedure

13. **Clish** Sentry. In the configuration mode, execute the following command for registration.

```
(config)#accs registration https://<FQDN of Access server><Admin Username of Access Server>
```

14. Enter the **Tenant password** and complete the registration.

15. In **Access**, click the **Sentry** tab.

16. Select the appropriate Sentry instance, then click **Action > Assign**.

17. Click **OK**.

18. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

```
(config)# accs config-fetch update
```

**Note:** All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

2. **Configure Access to create a Federated Pair.**



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://
alt.auto.mobileiron.com/acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIIDazCCAlOgAwIBAgIFAFIngxCeWdQYJKoZIhvcNAQELBQAwZDZlbnMlU2lnbmUzOjN1c2Qx
          QxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2Qx
          BgNVBAYTA1VTMB4XDTE3MDkyMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDEx
          luZ0N1c2QxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsM
          BgNVBAGMCKNhbm3JuaWEwEzA7BgNVBAYTA1VTMIBIjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEArsG5B5R9c9oK9s4
          7rXF12N+Kz27Bd26frt5jmAIRkz85j/C5o2HDXMOaPm+zZyE1cdJio1e5JVaoS+C/mzSckB19m+9QJf37H1+xht/
          IHhw4E0mt1Z1Baf+YTV8VYyhiQA2noAgSMK/hd1ibkMej1W/YNUk4HgZ1s5EBEtBNM80J20cohKQVqgn/21NBqC1Mr/
          VjYk15R1rMFQWdnI9Cyd0NZfzy9KgCBG9xElbzd0EGK9rAZQy/Caiwv3ySxqSxjxDsywb4f3hLW6TRI+z06Dk0q60nsDg/
          HQ0r/
          9RCvXjRSUyxcIHE61hne0+b5cfvoH1nmIdt3IQ95keL1EpuLwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAgaXmWzDhNHK8tbAm
          v3Hu9khL5EXsnKceprz6hzhVB7DOPY3p9hqzC7luz1M3vM3BfLirGh2BE8q3iFPj2M1LC+ibLDA1LrBtFEAKBrwL
          +TIgO9mOB7Bmai/tlJl$AoZzdCBaGd1dNlRrApTb1wj1+5JRdJ1D1GKYXkwlxhfw
          +zFf3nk7gWs5qNgj2qSKR8bdeZPH0jnQzjf5a9C+boNrLpnSHWVahRwWPyRza8WH3xut/C5JZdy/MOsKcK4T8nEUFawLOmiy
          +6SyX77Lzcc/HgrpN4y+7T043oyR0KrXdmifznQXbqhUvQLSuEcVe142reteLlt14GdX1UBh/410</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
alt.auto.mobileiron.com/acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://
alt.auto.mobileiron.com/acc/786900bf-fcf8-4488-bb8d-815080e667e5/idp"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Certificate

**SAML Issuer, Certificate, Global Logout Service URL (Logout Request destination), Global Logout Service URL (Logout Response destination), single sign on redirect service location**

3. Configure SSO settings as shown below on the Success Factors portal.

For SAML based SSO:

SAML v1.1 SSO  SAML v2 SSO

SAML Asserting Parties (IdP) MobileIron

Delete the asserting party Update the asserting party

SAML User Column

SAML Asserting Party Name

SAML Issuer

Company Phone

Contact Name

Contact Phone

Relying Party Description

Require Mandatory Signature

Enable SAML Flag

Login Request Signature (SF Generated/SP/RP):

SAML Profile

Enforce Certificate Valid Period

SAML Verifying Certificate Valid Period

SAML Verifying Certificate Status

SAML Verifying Certificate

Assertion

Browser/Post Profile

04/21/2017 - 04/14/2047

Certificate is valid.

```
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIFAFIngxCeWdQYJKoZIhvcNAQELBQAwZDZlbnMlU2lnbmUzOjN1c2Qx
QxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2Qx
BgNVBAYTA1VTMB4XDTE3MDkyMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDExMDE0NDEx
luZ0N1c2QxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsMB1N1c2QxQxEDA0BgNVBAsM
BgNVBAGMCKNhbm3JuaWEwEzA7BgNVBAYTA1VTMIBIjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEArsG5B5R9c9oK9s4
7rXF12N+Kz27Bd26frt5jmAIRkz85j/C5o2HDXMOaPm+zZyE1cdJio1e5JVaoS+C/mzSckB19m+9QJf37H1+xht/
IHhw4E0mt1Z1Baf+YTV8VYyhiQA2noAgSMK/hd1ibkMej1W/YNUk4HgZ1s5EBEtBNM80J20cohKQVqgn/21NBqC1Mr/
VjYk15R1rMFQWdnI9Cyd0NZfzy9KgCBG9xElbzd0EGK9rAZQy/Caiwv3ySxqSxjxDsywb4f3hLW6TRI+z06Dk0q60nsDg/
HQ0r/
9RCvXjRSUyxcIHE61hne0+b5cfvoH1nmIdt3IQ95keL1EpuLwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAgaXmWzDhNHK8tbAm
v3Hu9khL5EXsnKceprz6hzhVB7DOPY3p9hqzC7luz1M3vM3BfLirGh2BE8q3iFPj2M1LC+ibLDA1LrBtFEAKBrwL
+TIgO9mOB7Bmai/tlJl$AoZzdCBaGd1dNlRrApTb1wj1+5JRdJ1D1GKYXkwlxhfw
+ZfF3nk7gWs5qNgj2qSKR8bdeZPH0jnQzjf5a9C+boNrLpnSHWVahRwWPyRza8WH3xut/C5JZdy/MOsKcK4T8nEUFawLOmiy
+6SyX77Lzcc/HgrpN4y+7T043oyR0KrXdmifznQXbqhUvQLSuEcVe142reteLlt14GdX1UBh/410
-----END CERTIFICATE-----
```

**SAML v2 : SP-initiated logout**

Support SP-initiated Global Logout

Yes ▾

SP sign LogoutRequest

No ▾

SP validate LogoutResponse

No ▾

Global Logout Service URL (LogoutRequest destination)

<https://alt.auto.mobileiron.com/acc/dad0e42>**SAML V2 : IDP-initiated Global Logout**

SP validate LogoutRequest signature

Yes ▾

SP sign LogoutResponse

Yes ▾

Global Logout Service URL (LogoutResponse destination)

<https://alt.auto.mobileiron.com/acc/dad0e42>**SAML v2: Login Response with Http artifact binding**

Artifact Resolution Service Location (supplied by idp):

Require ArtifactResolve Signature (sp to idp)

No ▾

Require ArtifactResponse Signature (idp to sp)

No ▾

**SAML v2: NameID Setting**

Require sp must encrypt all NameID elements

No ▾

NameID Format

unspecified ▾

**SAML v2 : SP-initiated login**

Enable sp initiated login (AuthnRequest)

Yes ▾

Default issuer

single sign on redirect service location (to be provided by idp)

<https://auto.mobileiron.com/acc/dad0e42>

Send request as Company-Wide issuer

No ▾

## Verification

SuccessFactors Mobile App follows Activation process for the user to activate the profile. There are three kinds of Activation process. These processes do not support SAML SSO flow.

1. Activation Code
2. QR Code



## Activation

Please activate your profile by selecting one of the activation methods below:

Use Activation Code

Scan QR Code

Try Demo

### 3. Email based Activation

- Download the SuccessFactors mobile application on the device.
- From safari on iOS and chrome on Android, Access the URL mentioned in step 2 in the email.  
It prompts to open the link in Mobile App on iOS. Click Ok.  
On Android, everything is seamless. This starts the SAML SSO flow.



Copyright © 2016 - 2018 MobileIron, Inc. All Rights Reserved.

Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.